

AO 106 (Rev. 7/10) Affidavit for Search
Warrant

AUSA Elie Zenner, (312) 697-4032

FILED
11/12/2024**TD**THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

In the Matter of the Search of:

Case No.

The cellular telephone further described in
Attachment A

Ref. No. 23 R 657

24M880**APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT**

I, Dustin Gourley, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachments A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence.

The search is related to a violation of:

Code Section

Title 18, United States Code, Section 924(c)
Title 18, United States Code, Section 2119
Title 18, United States Code, Section 922(g)

Offense Description

Using a firearm during a crime of violence
Carjacking
Felon in Possession of a Firearm

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

Dustin Gourley
Applicant's Signature

DUSTIN GOURLEY, Special Agent
Federal Bureau of Investigation

Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: November 12, 2024

Beth W. Jantz
Judge's signature

City and State: Chicago, Illinois

BETH W. JANTZ, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Dustin Gourley, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately 2012.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to violate crimes, such as kidnapping, bank robbery, robberies, carjackings, and the apprehension of violent fugitives. I have participated in the execution of multiple federal search warrants, including for information from a cellular phone.

3. This affidavit is made in support of an application for a warrant to search a black Apple cellular telephone (**Subject Phone 1**) and a white Apple cellular telephone (**Subject Phone 2**) (collectively, "**Subject Phones**") described further in Attachment A, for evidence and instrumentalities described further in Attachment B, concerning using a firearm during a crime of violence, possession of a firearm by a prohibited person, and carjacking offenses, in violation of Title 18, United States Code, Sections 924(c), 922(g), and 2119 (the **Subject Offenses**).

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included

each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 924(c), 922(g), and 1951 are located within the **Subject Phones**.

I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT PHONES

A. Summary

5. On January 31, 2024, a grand jury in the Northern District of Illinois indicted JAVON STINGLEY and three co-defendants for conspiracy to commit carjackings and multiple counts of carjacking and using a gun in furtherance of crimes of violence in 24-CR-55. Law enforcement attempted to arrest STINGLEY, but as of October 2024, STINGLEY was not in custody. On October 13, 2024, STINGLEY was arrested after he and two others fled from a Ford Explorer (the “**Subject Vehicle**”) that was taken during a carjacking on October 6, 2024. The **Subject Phones** were recovered from the front driver and passenger seat areas of the **Subject Vehicle**.

B. Facts Supporting Probable Cause

Previous Carjacking Indictment of STINGLEY

6. On January 31, 2024, JAVON STINGLEY and three co-defendants were indicted in the Northern District of Illinois in 24-CR-55, for conspiracy to commit carjackings (Count One) and using a gun to carjack a Dodge Challenger on February 19, 2023 (Counts Three and Four).

7. During its investigation into the carjackings charged in 24-CR-55, agents recovered relevant evidence from a phone used by STINGLEY's co-defendant MICHAEL BANKS, including (1) pictures of carjacked vehicles with STINGLEY, BANKS, and their co-defendants; (2), pictures of guns, and (3) text messages and call records between BANKS and STINGLEY, including evidence of communication shortly before the February 19, 2023, carjacking that STINGLEY is charged with in Counts Three and Four.

8. In addition to that evidence, agents also obtained cell tower records relating to phone numbers associated with the four defendants. Those cell tower records showed, among other things, that a phone associated with STINGLEY's Cash App account was in the area of the February 19, 2023, carjacking at the approximate time of the carjacking.

9. After the grand jury returned the indictment on January 31, 2024, FBI agents took BANKS and JOSEPH SMITH into custody, but were unable to locate STINGLEY and GARY LUELLEN, the remaining co-defendants. During agents' attempts to locate STINGLEY, they went to STINGLEY's last known residence in Calumet Park, IL, and spoke to his grandparents, informing the grandparents that a warrant was issued for STINGLEY's arrest.

10. According to phone records for STINGLEY's then-known phone number, the phone was no longer active after approximately July 9, 2023.

11. According to law enforcement databases, STINGLEY is a felon as a result of prior felony convictions, including for Aggravated Unlawful Use of a Weapon and Intent to Deliver a Controlled Substance.

October 2024: Stingley is Arrested in Carjacked Vehicle

12. According to Chicago Police Department reports, on October 6, 2024, Victim A and Victim B were carjacked by two unknown offenders. Victim A reported to police that on October 6, 2024, Victim A and Victim B were sitting in Victim A's 2016 Ford Explorer bearing Illinois license plate ER99851 (the **Subject Vehicle**) while parked at about 8240 South Stony Island in Chicago. Two unknown black male offenders approached the driver door and passenger door and one of the offenders knocked on the driver-side window and stated words to the effect of, "If you get out of the car I won't shoot you."

13. According to police reports, Victim A and Victim B exited the **Subject Vehicle** because the carjackers implied that they had a weapon. The two offenders got into the Explorer and fled. Victim A stated that her Apple iPhone 13, groceries, and Apple Air Pods were stolen along with the **Subject Vehicle**.

14. According to Calumet City Police reports, on October 13, 2024, police officers were in the area of Sibley Boulevard and Torrence Avenue in Calumet City, when they received an alert from a License Plate Reader camera that a stolen vehicle with Illinois license plate ER99851 (the **Subject Vehicle**), was captured on camera at Sibley Boulevard and Madison Avenue in Calumet City.

15. According to police reports, officers located the **Subject Vehicle** parked in a parking lot at about 4 Sibley Boulevard in Calumet City. Officers activated the emergency lights on their police vehicles and attempted to block in the **Subject Vehicle**.

16. Three occupants exited the **Subject Vehicle** and fled on foot. Officers observed that one of the three occupants was a black male with dreadlocks and an orange sweatshirt, later identified as STINGLEY. STINGLEY was sitting in the driver's seat of the **Subject Vehicle** before fleeing. After a short foot pursuit lasting approximately two minutes, officers detained STINGLEY.

17. STINGLEY initially identified himself as "Taurean McKay." When officers ran his identifying information through law enforcement databases, however, they learned that he was JAVON STINGLEY. In addition to the active federal arrest warrant related to 24-CR-55, STINGLEY also had an active arrest warrant from Iowa.

18. Officers conducted a post-*Miranda* interview of STINGLEY. STINGLEY stated that on October 13, 2024, he was with someone named "Four," and they drove around in a Mazda vehicle before getting into the **Subject Vehicle**. STINGLEY admitted that he was driving the **Subject Vehicle** and had the key fob to the vehicle. STINGLEY admitted to fleeing from the **Subject Vehicle** when police activated their lights and stated that "Four" told him the **Subject Vehicle** was stolen while they were fleeing.

19. According to police reports, officers recovered from STINGLEY's person the following: (1) the key fob to the **Subject Vehicle**; (2) 6 yellow capsules containing a white crystal-like powdery substance; and (3) one white circular pill with an "M" imprinted on one side and "0052" imprinted on the other.

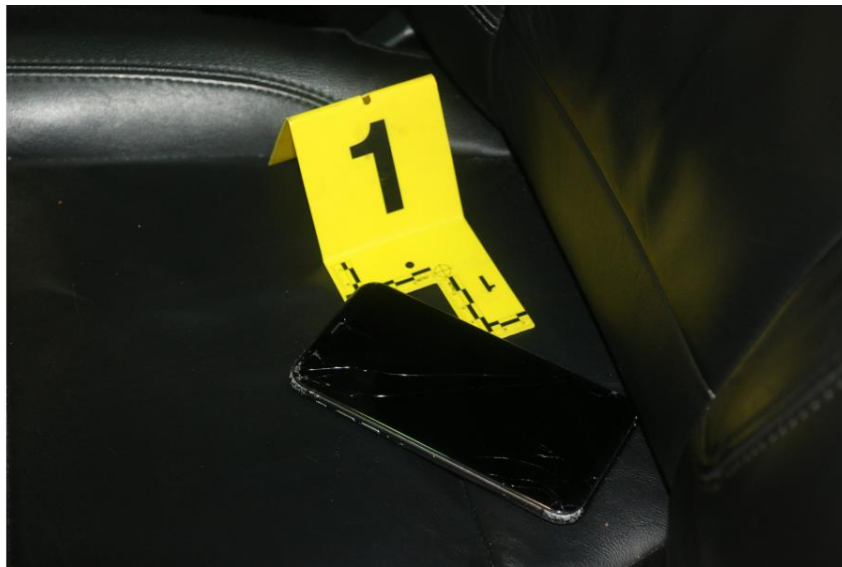
20. STINGLEY did not have a cellular telephone on his person at the time of his arrest.

21. According to police reports, officers also detained another person who fled from the vehicle. This second occupant identified himself as RANGER MILLER and spontaneously yelled "I was in the back!" as he was being detained.

22. Officers conducted a post-*Miranda* interview of MILLER. MILLER stated that on October 13, 2024, he was walking when he was picked up in the **Subject Vehicle** by the brother of a female friend of his. MILLER said he did not know who was driving the **Subject Vehicle** and only knew the other passenger as "Tay-Tay."

23. Officers recovered a black handgun on the driver's-side floorboard of the **Subject Vehicle**.

24. After the **Subject Vehicle** was towed, Victim A consented to police's search of the **Subject Vehicle**. During the subsequent search, police recovered a black iPhone with a cracked screen (**Subject Phone 1**) on the driver's seat of the **Subject Vehicle**. Below are photographs of the phone on the driver's seat:



25. During the search law enforcement also recovered a white iPhone (Subject Phone 2) from the front passenger door area. Below is a photograph of Subject Phone 2:



26. Victim A stated that the **Subject Phones** did not belong to her or Victim B.

27. Since October 13, 2024, the above-described **Subject Phones** have been in the custody of the Chicago Police Department.

28. Through experience as a law enforcement officer and through the experience of other law enforcement officers as conveyed to me, I have learned that individuals involved in carjacking offenses commonly use cellular telephones as a means to communicate in order to coordinate their activities before, during, and after a carjacking. More specifically with respect to STINGLEY and his associates, I know that, as described above, STINGLEY and BANKS communicated by text message and phone call in the hours before the February 19, 2023, carjacking charged in 24-CR-55. Although available evidence indicates that STINGLEY is no longer using the specific phone he used in connection with the charged carjackings, that evidence

further supports probable cause to believe he continued to use cellular phones in connection with his continued illegal activity.

29. Individuals involved in criminal offenses also often store telephone numbers and names or nicknames of fellow conspirators on their telephones and the telephones also reflect recent call history. Finally, individuals often use text messaging and digital photographs in furtherance of their criminal activity that are stored on cellular telephones. Based upon my training and experience, I know that cellular phones may contain relevant evidence of the offenses, including text messages made or received from the **Subject Phones** that are located in the memory of the **Subject Phones**, which messages may provide information regarding the identities of, and the methods and means of operation and communication used by, the participants in the offenses. Moreover, digital photographs located in the memory of the **Subject Phones** may contain images of the tools or participants involved in the offenses. Moreover, digital photographs stored in the **Subject Phones** may contain images of the user of the **Subject Phones**, the user's associates (including persons involved in or knowledgeable about the subject offenses), places frequented by the user of the phone leading up to and during the subject offenses, and locations and instrumentalities used in committing the subject offenses.

30. In addition, based on my training and experience, I know that information stored within a cellular phone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus

enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cell phone can indicate who has used or controlled the cell phone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the cell phone at a relevant time. Further, such stored electronic data can show how and when the cell phone and its related account were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cell phone access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cell phone account owner.

31. Additionally, information stored within a cell phone may indicate the geographic location of the cell phone and user at a particular time (*e.g.*, location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the cell phone owner’s state of mind as it relates to the offense under investigation. For example, information in the cell phone may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by

breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely.

32. In addition, for all the reasons described above, there is also probable cause to believe that the **Subject Phones** will contain evidence of STINGLEY's attempts to evade arrest, which is evidence of his consciousness of guilt in case 24 CR 55, in that location information, text messages, images, and other data can provide evidence of STINGLEY's location, knowledge of the warrant for his arrest, and identify persons who assisted him in evading arrest.

33. Because, as explained above, the **Subject Phones** are associated with the target in this case, because there was telephonic communication between participants involved in the offenses, and because, in my experience and in the experience of other agents, defendants use telephones to contact co-conspirators, there is probable cause to believe the **Subject Phones**, described further in Attachment A, contain evidence of violations of using a firearm during a crime of violence, possession of a firearm by a prohibited person, and carjacking offenses.

II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

34. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most

or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

35. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

36. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

37. The warrant I am applying for would permit law enforcement to obtain from **JAVON STINGLEY** the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock **Subject Phone 1**. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that **Subject Phone 1** offers users the ability to unlock the device through biometric features, namely, facial recognition features, in lieu of a numeric or alphanumeric passcode or password.

b. **Subject Phone 1** is an Apple product with a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock the device. Once a fingerprint is registered, a user can unlock the device by pressing

the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device.

c. **Subject Phone 1** is an Apple product with a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric feature(s) because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. The passcode or password that would unlock **Subject Phone 1** is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials published by device

manufacturers, that **Subject Phone 1's** biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, because **Subject Phone 1** is a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Based on these facts and my training and experience, as well as the location of the recovery of **Subject Phone 1**, it is likely that **Subject Phone 1** belongs to STINGLEY and thus that his biometric characteristics are among those that are able to unlock the **Subject Phone 1**.

h. Due to the foregoing, the warrant I am applying for would permit law enforcement personnel to press or swipe the fingers (including thumbs) of **JAVON STINGLEY** to the fingerprint scanner of the **Subject Phone 1**¹ and/or hold the device in front of the face of **JAVON STINGLEY** and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

¹ Law enforcement will select the fingers to depress to the fingerprint scanner to avoid compelling the user of the device to disclose information about his or her knowledge of how to access the device.

III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

38. The government's review of electronic storage media, including cell phones, already in its possession shall be conducted pursuant to the following protocol.

39. The review of electronically stored information and electronic storage media described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

a. examination of categories of data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

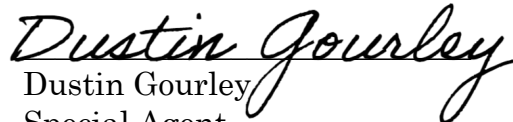
d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B; and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

IV. CONCLUSION

40. Based on the above information, I respectfully submit that there is probable cause to believe that offenses, in violation of Title 18, United States Code, Sections 922(g), 2119, and 924(c), have been committed, and that evidence relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Phones**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the **Subject Phones** more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.


Dustin Gourley
Special Agent
Federal Bureau of Investigation

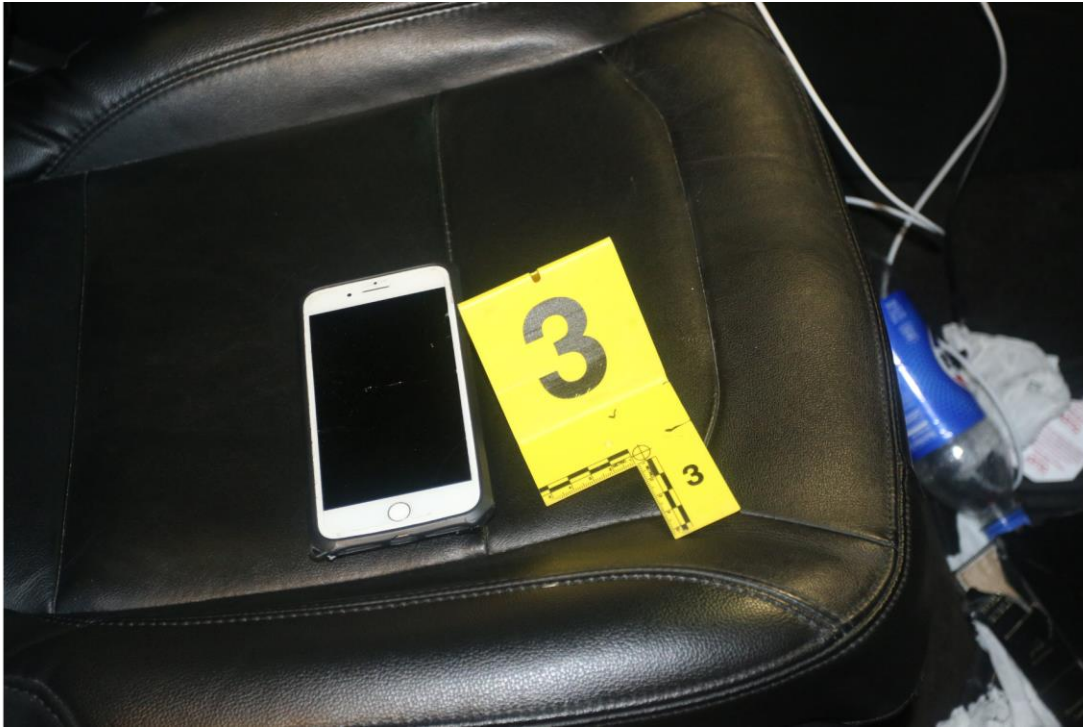
Sworn to and affirmed by telephone 8th day of November, 2024

Honorable BETH W. JANTZ
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

A white Apple iPhone, as depicted below:



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence concerning violations of Title 18, United States Code, Sections 922(g), 2119, and 924(c), as follows:

1. All items, including names, aliases, and numbers, including the number associated with the **Subject Phones** and any number directory stored in the memory of the **Subject Phones**, that provides information regarding the user of the phones and identities of the participants and/or coconspirators involved in the **Subject Offenses**.

2. All telephone calls and voicemails made or received that provide information regarding the identities of and the methods and means of operation and communication by the participants and/or coconspirators involved in the **Subject Offenses**.

3. All text messages made or received that provide information regarding the identities of and the methods and means of operation and communication by the participants and/or coconspirators involved in the **Subject Offenses**.

4. All data from October 1, 2024 through October 13, 2024 that might identify the physical location of the users of the **Subject Phones** during the planning, commission, or concealment of the **Subject Offenses**.

5. All digital photographs, videos, audio recordings, and social media that provide information regarding the instrumentalities used in the **Subject Offenses**, the identities of and the methods and means of operation and communication by the

participants and/or coconspirators involved in the **Subject Offenses**, associates of the user, or users, of the **Subject Phones**, and areas frequented by the user, or users, of the **Subject Phones** during the planning, commission, and concealment of the **Subject Offenses**.

6. All data concerning social media accounts located in the memory of the **Subject Phones** that provide information regarding the identities of and the methods and means of operation and communication by the participants and/or coconspirators involved in the **Subject Offenses**.

7. All financial information located in the memory of the **Subject Phones** that provides information regarding the identities of participants and/or coconspirators involved in the **Subject Offenses**, as well as transfers of funds related to the **Subject Offenses**.

8. All data from February 20, 2024 to October 13, 2024 located in the memory of the **Subject Phones** related that provides evidence of STINGLEY's location, knowledge of the warrant for his arrest, and the identity persons who assisted him in evading arrest.

ADDENDUM TO ATTACHMENT B

The government's review of electronic storage media, including cell phones, already in its possession shall be conducted pursuant to the following protocol:

The government must make reasonable efforts to use methods and procedures that will locate those categories of data, files, documents, or other electronically stored information that are identified in the warrant, while minimizing exposure or examination of categories that will not reveal the items to be seized in Attachment B.

The review of electronically stored information and electronic storage media described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

a. examination of categories of data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B; and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

Law enforcement personnel are not authorized to conduct additional searches for any information beyond the scope of the items to be seized by this warrant as set forth in Attachment B. To the extent that evidence of crimes not within the scope of this warrant appears in plain view during the government's review, the government shall submit a new search warrant application seeking authority to expand the scope of the search prior to searching portions of that data or other item that is not within the scope of the warrant. However, the government may continue its search of that

same data or other item if it also contains evidence of crimes within the scope of this warrant.